

Oracle Separation of BQP and PH

Cody Jordan

Michael Cash

Mehdi Ardebili

The "Oracle Separation of BQP and PH" is strong evidence towards a fundamental difference between quantum and classical computing. This paper presents a particular problem, forrelation, as an oracle problem which can separate the two complexity classes. This problem asks a computer to distinguish between values drawn from a uniform distribution against those drawn from a distribution where some elements are correlated based on the Hadamard transform. The separation is carried out by showing that an efficient quantum algorithm is able to distinguish these distributions while no classical circuit in the complexity AC^0 is. From this they establish that even alternating Turing machines, those capable of addressing problems in the polynomial hierarchy (PH) are unable to address a problem which a quantum computer can.